Kişisel Verilerin Korunması

Türkiye I Avrupa Birliği I Birleşik Krallık I Küresel

2025

Shape the future with confidence

Veri Koruma I Türkiye

2024'ü bitirirken...

19 Aralık 2024 I Kişisel Verileri Koruma Kurumu, "Kabahatlerin Zaman Bakımından Uygulanması Bilgi Notu" başlıklı belgeyi yayımladı.

Kişisel Verileri Koruma Kurumu, yurt dışı veri aktarımı ve özel nitelikli kişisel verilere dair KVKK değişikliklerine istinaden "Kabahatlerin Zaman Bakımından Uygulanması Bilgi Notu" belgesini yayımladı.

Bilgi notuyla, kabahat niteliğindeki eylemlerin işlendiği tarihle Kişisel Verileri Koruma Kurumu'na yapılan şikayet başvuru tarihi ve Kurul kararının verileceği zaman arasındaki farklara ilişkin Kanun'un zaman bakımından uygulanmasına dair belirsizliklerin açıklanması amaçlanmaktadır.

Bilgi notu içeriğinde, Kanun'un zaman bakımından uygulanması ile ilgili bir tablo mevcuttur.

İlgili bilgi notuna buradan ulaşabilirsiniz.

2025'in ilk çeyreği...

2 Ocak 2025 I Kişisel Verilerin Yurt Dışına Aktarılması Rehberi yayımlandı. (1/2)

12 Mart 2024 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe giren 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ("7499 sayılı Kanun") çerçevesinde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("KVKK") "Kişisel Verilerin Yurt Dışına Aktarılması" başlıklı 9. maddesinde değişiklikler meydana gelmiştir. Yeni düzenlemenin uygulamasında yol göstermek adına Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'in ("Yönetmelik") 10.07.2024 tarihli ve 32598 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmesinin ardından 2 Ocak 2025 tarihinde Kişisel Verilerin Yurt Dışına Aktarılması Rehberi ("Rehber") Kişisel Verileri Koruma Kurumu'nun ("Kurum") internet sitesinde yayımlanmıştır.

Rehber'de; değişikliklerin amacı ve gerekçesi, hangi aktarımların KVKK madde 9 uyarınca yurt dışına aktarım olarak kabul edildiği, standart sözleşmeler başta olmak üzere kişisel verilerin yurt dışına aktarılması bakımından öngörülen mekanizmaların nasıl uygulanması gerektiği ve KVKK uyarınca kişisel verilerin yurt dışına aktarımının mümkün olduğu istisnai aktarım hallerine ilişkin açıklamalara yer verilmiştir.

Türkiye'de yeterlilik kararı verilmiş ülke veya sektör listesinin henüz yayınlanmamış olması nedeniyle yurt dışına kişisel veri aktarımlarında uygun güvencelere dayalı aktarım metotları uygulama alanı bulmaktadır. Rehber'de de KVKK ve Yönetmelik'te yer alan düzenlemelere ek olarak, uygun güvencelere dayalı aktarım metotlarının uygulamasına yönelik daha detaylı yönlendirmeler yapılmıştır. Bağlayıcı şirket kurallarında yer alması gereken asgari unsurlara ve standart sözleşme eklerinin nasıl doldurulması gerektiğine ilişkin açıklamalara yer verilmiştir. Aktarım mekanizmalarına ilişkin olarak Rehber'de aşağıdaki hususlar detaylandırılmıştır:

2 Ocak 2025 I Kişisel Verilerin Yurt Dışına Aktarılması Rehberi yayımlandı. (2/2)

- **Bağlayıcı şirket kuralları**: Yönetmelik'in 13. maddesinde bağlayıcı şirket kurallarında yer alması gereken asgari unsurlar düzenlenmiş, Rehber'de de asgari unsurlar tablo usulü ile detaylı olarak açıklanmıştır. Bağlayıcı şirket kurallarının Kişisel Verileri Koruma Kurulu ("Kurul") tarafından onaylanması gerekmektedir. Rehber'de ortak ekonomik faaliyette bulunan teşebbüs grubunun Türkiye'de yerleşik olup olmamasına göre bağlayıcı şirket kurallarına başvuru usulüne yönelik detaylı yönlendirmelerde bulunulmuştur.

- **Standart sözleşmeler**: Kurul tarafından bir izin/onay alınmasına gerek olmaması nedeniyle standart sözleşmelere dayalı aktarım uygulamada en çok tercih edilen uygun güvence çeşididir. Kurul tarafından yayımlanan standart sözleşmelerin veri aktaran taraflar tarafından doldurulmasında oluşan soruların cevaplandırılması adına Rehber'de standart sözleşmelerin eklerinin doldurulmasına yönelik açıklamalara yer verilmiştir. Ayrıca, KVKK ve Yönetmelik'te standart sözleşmeler için Türkçe metnin esas alınacağının belirtilmiş olması nedeniyle sözleşmenin çift sütun olarak, başka bir deyişle iki dilde hazırlanıp hazırlanamayacağına ilişkin tartışmalar meydana gelmiştir. Rehber'de, Kurum'a çift sütunlu olarak ve Türkçe ile diğer başka bir dilde düzenlenmiş standart sözleşmelerin bildirilmesi suretiyle Kanun'un 9. maddesinin dördüncü fıkrasının (c) bendi ile beşinci fıkrasında öngörülen gerekliliklerin karşılanabileceğinin belirtilmesi ile bu soru işareti ortadan kaldırılmıştır. Uygulamada ayrıca, standart sözleşmelerin bildirilmesi esnasında Kurum'a sunulması gereken yetki belgelerinde apostil gerekliliği de tartışma alanı bulmuştur. Rehber'de ayrıksı bir düzenlemenin veya uluslararası anlaşmanın yokluğu halinde Yabancı Resmi Belgelerin Tasdiki Mecburiyetinin Kaldırılması Sözleşmesine taraf bir ülkede düzenlenmiş resmi belgeler Kurum'a sunulurken apostil şerhinin bulunması gerektiği belirtilerek bu tartışmaya son verilmiştir.

- **İstisnai aktarımlar**: İstisnai aktarımlar veya KVKK'daki tanımı ile arızi aktarımlar yeterlilik kararının bulunmaması ve dördüncü fıkrada öngörülen uygun güvencelerden herhangi birinin sağlanamaması durumunda, KVKK'da sayılan arızi aktarım hallerinde yurt dışına veri aktarımlarının gerçekleştirilebileceği durumlar olarak öngörülmüştür. Rehber'de aktarımın arızi olarak kabul edilmesi için işbu aktarımın veri aktaranın olağan faaliyet akışı içerisinde yer alıp almadığının değerlendirilmesinin önem arz ettiği, aktarımın kaç kere gerçekleştiğinden bağımsız olarak değerlendirme yapılması gerektiği belirtilmiştir. Olağan faaliyet akışı içinde yapılan aktarımlar arızi aktarım olarak kabul edilmemektedir.

Rehber ile KVKK'da meydana gelen değişiklikler sonucunda kişisel verilerin yurt dışına aktarılmasında meydana gelen problemlere yönelik açıklamalarda bulunulmuştur, meydana gelen sorulara yönelik örneklere yer verilmiştir.

İlgili Rehbere buradan ulaşabilirsiniz.

Veri Koruma I Türkiye

3 Ocak 2025 I 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İdari Para Cezası Tutarları yayımlandı.

KVKK'nın "Kabahatler" başlıklı 18. maddesi uyarınca idari yaptırımlar öngörülmüştür. İdari yaptırımlar, her yıl yeniden değerleme oranına göre artırılmaktadır. 2025 yılına yönelik miktarlar Kurum'un internet sitesinde ilan edilmiştir ve aşağıda yer almaktadır;

- Aydınlatma yükümlülüğüne aykırılık halinde 68.083 TL – 1.362.021 TL,
- Veri güvenliğine ilişkin yükümlülüklere aykırılık halinde 204.285 TL – 13.620.402 TL,
- Kurul tarafından verilen kararları yerine getirmeme halinde 340.476 TL – 13.620.402 TL,
- Veri Sorumluları Siciline (VERBİS) kayıt ve bildirim yükümlülüğüne aykırı hareket etme halinde 272.380 TL – 13.620.402 TL,
- KVKK'nın 9. maddesinin beşinci fıkrasında öngörülen bildirim yükümlülüğüne aykırılık halinde 71.965 TL – 1.439.300 TL.

İdari para cezalarına ilişkin tabloya buradan ulaşabilirsiniz.

6 Ocak 2025 I Sermaye Piyasası Kurulu ile Kişisel Verileri Koruma Kurumu arasında "İş birliği ve Bilgi Paylaşımı Protokolü" imzalandı.

SPK ile Kurum arasında İş Birliği ve Bilgi Paylaşımı Protokolü'nün ("Protokol") imzalandığı bildirilmiştir. Protokol ile sermaye piyasalarında kişisel verilerin işlenmesi ve korunması konularında artan ihtiyaçlar doğrultusunda, iki kurum arasında etkin bir koordinasyon ve iş birliğinin sağlanmasının hedeflendiği belirtilmiştir. Protokol, her iki kurumun görev alanına giren ortak konularda bilgi ve görüş paylaşımı yapılmasını ve bu çerçevede; kişisel verilerin korunması, veri mahremiyeti ve veri güvenliği konularında ortak projeler ve çalışmaların gerçekleştirilmesini, meslek personelinin yetiştirilmesini, ortak yayınlar ve farkındalık artırıcı etkinliklerin düzenlenmesini içermektedir.

8 Ocak 2025 I Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi güncellendi.

Bankacılık faaliyetleri kapsamında, bankalar tarafından çeşitli kanallar üzerinden yoğun bir biçimde kişisel veri işlenmesi nedeniyle Kişisel Verileri Koruma Kurumu ("Kurum") ile Türkiye Bankalar Birliği iş birliğiyle hazırlanan Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulama Rehberi ("İyi Uygulamalar Rehberi") 5 Ağustos 2022 tarihinde yayımlanmıştır. 12 Mart 2024 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe giren 7499 Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda ("KVKK") kişisel verilerin yurt dışına aktarımı ve özel nitelikli kişisel verilerin işlenmesine yönelik gerçekleştirilen değişiklikler göz önüne alınarak İyi Uygulamalar Rehberi güncellenmiştir.

Güncellenen İyi Uygulamalar Rehberi'ne buradan ulaşabilirsiniz.

Veri Koruma I Türkiye

13 Ocak 2025 I Arabuluculuk Faaliyetleri Kapsamında Aydınlatma Yükümlülüğünün Yerine Getirilmesine İlişkin Kamuoyu Duyurusu Kurum'un internet sitesinde yayımlandı.

Arabulucuların KVKK'nın uygulanması bakımından veri sorumlusu sıfatını haiz olup, veri sorumlusunun yükümlülüklerine tabi oldukları belirtilmiştir. 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu'nun ("6325 sayılı Kanun") Tarafların aydınlatılması" başlıklı 11. maddesinde ise "Arabulucu, arabuluculuk faaliyetinin başında, tarafları arabuluculuğun esasları, süreci ve sonuçları hakkında gerektiği gibi aydınlatmakla yükümlüdür." hükmü düzenlenmiştir. Kurum, 6325 sayılı Kanun'da düzenlenen aydınlatma yükümlülüğüyle KVKK'da düzenlenen aydınlatma yükümlülüğünün farklılık arz ettiğini belirtmiştir. Bu çerçevede, 6325 sayılı Kanun'un 11. maddesi uyarınca arabuluculuk faaliyetinin başında arabulucu tarafından arabuluculuğun esasları, süreci ve sonuçları hakkında taraflara bilgi verilmesinin KVKK'nın 10. maddesinde düzenlenen aydınlatma yükümlülüğünün yerine getirildiği anlamına gelmediği, arabuluculuk faaliyetleri kapsamında işlenen kişisel verilere ilişkin arabulucu tarafından KVKK'nın 10. maddesinde sayılan hususlarda ilgili kişilere ayrıca bilgi verilmesi suretiyle aydınlatma yükümlülüğünün yerine getirilmesi gerektiğine değinilmiştir.

İlgili Kamuoyu Duyurusuna buradan ulaşabilirsiniz.

5 Şubat 2025 I Yurt Dışına Kişisel Veri Aktarımında Kullanılacak Standart Sözleşmelerde Dikkat Edilmesi Gereken Hususlara İlişkin Kamuoyu Duyurusu, Kurum'un internet sitesinde yayımlandı. (1/2)

Yurt dışına kişisel veri aktarımına ilişkin Kurum'a iletilen Standart Sözleşmelerin incelenmesi neticesinde tespit edilen ve dikkat edilmesi gereken hususlarla, Kurum tarafından belirtilerek imzalanacak olan standart sözleşmelerde meydana gelebilecek problemlerin önüne geçilmesi amaçlanmıştır. Kurum tarafından aşağıdaki hususlar vurgulanmıştır:

- Standart sözleşmelerde tarafları temsile ve imzaya yetkili kişilerin ikisinin de geçerli imzasının bulunması gerekmektedir.
- İmzaların 6098 sayılı Türk Borçlar Kanunu'nun imzaya ilişkin düzenlemelerine uygun olması gerekmektedir.
- Çift dilde ve çift sütunlu olarak imzalanan sözleşmelerde Türkçe metnin altında mutlaka iki tarafın da imzası bulunmalıdır.
- Sözleşmeyi imzalayan kişilerin temsile ve imzaya yetkili olduklarına dair tevsik edici belgelerde sözleşmeyi imzalayan kişilerin isimlerinin yer almaması halinde sözleşme yetkisiz kişiler tarafından imzalanmış olacağından standart sözleşme geçerli sayılmamaktadır.
- Standart sözleşme metnindeki taraf isimlerinde eksiklik olmaması gerekmektedir.
- Aktarım taraflarının her ikisinin de imza tarihleri standart sözleşme metni üzerinde belirtilmelidir.
- Aktarım taraflarının adres, irtibat noktası, imzacı isimleri veya benzeri bilgilerinin standart sözleşme metninde açıkça belirtilmesi gerekmektedir.
- Standart sözleşmenin sayfalarında eksik bulunmaması gerekmektedir.
- İstisnai bir düzenlemenin veya uluslararası anlaşmanın yokluğu halinde Yabancı Resmi Belgelerin Tasdiki Mecburiyetinin Kaldırılması Sözleşmesine taraf bir ülkede düzenlenmiş resmi belgelerin apostil şerhi ile birlikte Kuruma sunulması gerekmektedir.

Veri Koruma I Türkiye

5 Şubat 2025 I Yurt Dışına Kişisel Veri Aktarımında Kullanılacak Standart Sözleşmelerde Dikkat Edilmesi Gereken Hususlara İlişkin Kamuoyu Duyurusu, Kurum'un internet sitesinde yayımlandı. (2/2)

- Kuruma sunulacak tevsik edici belgeler ile yabancı dildeki her belgenin, noter onaylı Türkçe çevirisi ile birlikte sunulması gerekmektedir.
- Standart sözleşmede, aktarım taraflarının imzaları daha ileri bir tarihte tamamlanmış olmasına rağmen sözleşmenin geçmişe dönük olarak yürürlüğe gireceğine dair 'yürürlük tarihi:...' ve benzeri ibarelere yer verilmemelidir.
- Aktarım taraflarının, kişisel veri aktarımı bağlamında uygun standart sözleşme tipini belirledikten sonra yalnızca seçimlik veya alternatif içerikli standart sözleşme maddeleri üzerinde değişiklik yapabilmeleri mümkündür.

İlgili Kamuoyu Duyurusuna buradan ulaşabilirsiniz.

26 Şubat 2025 I Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Rehber, Kurum'un internet sitesinde yayımlandı.

7499 sayılı Kanun ile KVKK'nın özel nitelikli kişisel verilerin işlenmesini düzenleyen 6. maddesinde değişiklik yapılmış olup değişiklik ile mevcut olan özel nitelikli kişisel veri işleme şartlarına yeni veri işleme şartları, başka deyişle hukuka uygunluk sebepleri getirilmiştir. İşbu değişikliğe ek olarak söz konusu değişlik ile istihdam, iş sağlığı ve güvenliği ve sosyal güvenlik gibi alanlarda, açık rıza olmasa dahi, ilgili şartlar sağlandığı takdirde kişisel verilerin işlenmesi mümkün kılınmıştır. Bu çerçevede, özel nitelikli kişisel verilerin işlendiği durumlarda veri sorumlularının doğru hukuki sebeplere dayalı olarak özel nitelikli kişisel veri işlemeleri ve Kanun'a uygun şekilde yükümlülüklerini yerine getirmeleri için yol gösterici olması amacıyla Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Rehber Kurul tarafından yayımlanmıştır.

Rehber ile öncelikle özel nitelikli kişisel veriler, özel nitelikli kişisel verilerin işlenme şartları ve değişiklikler kapsamında KVKK'ya uyum sağlanması adına veri sorumlularınca yapılması gerekenlere değinilmiştir. Değişiklikler kapsamında veri sorumlularınca kişisel veri işleme envanterinin güncellenmesi, açık rıza alınması süreçlerinin düzenlenmesi, aydınlatma metinlerinde gerekli değişikliklerin yapılması, saklama ve imha politikasının güncellenmesi ve veri güvenliği tedbirlerinin alınması gerektiği belirtilmiştir.

İlgili Rehbere buradan ulaşabilirsiniz.

13 Mart 2025 I Taahhütname Başvurusu Hakkında Duyuru, Kurum'un internet sitesinde yayımlandı.

KVKK'nın 9. maddesinde hakkında yeterlilik kararı bulunmayan ülkelere veri aktarımının KVKK'nın 5. ve 6. maddelerde belirtilen şartlardan birinin varlığı, ilgili kişinin aktarımın yapılacağı ülkede de haklarını kullanma ve etkili kanun yollarına başvurma imkânının bulunması kaydıyla, 9. maddede belirtilen uygun güvencelerden birinin taraflarca sağlanması halinde gerçekleştirilebileceği belirtilmiştir. 9. Maddede öngörülen uygun güvencelerden biri de yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı ve Kurul tarafından aktarıma izin verilmesidir.

Kurum'a sunulan üç adet Taahhütname başvurusunun, Kurul tarafından KVKK'nın 9. maddesinin dördüncü fıkrasının (ç) bendi kapsamında değerlendirilerek 12.03.2025 tarihinde Kurul tarafından söz konusu veri aktarımlarına izin verildiği duyurulmuştur.

İlgili duyuruya buradan ulaşabilirsiniz.

Veri Koruma I Avrupa Birliği I Birleşik Krallık

14 Ocak 2025 I Fransa'nın veri koruma otoritesi CNIL, mobil uygulamalarda kullanıcılardan talep edilen veri paylaşım izinlerine dair uyulması gereken kurallara yönelik bir içerik yayımladı.

Fransa'nın veri koruma otoritesi Commission Nationale de l'Informatique et des Libertés (CNIL), mobil uygulamalarda kullanıcıların veri paylaşım izinlerine dair yeni öneriler yayımlamıştır. Bu öneriler, mobil uygulamaların kullanıcıların kişisel verilerini daha güvenli bir şekilde toplamasını sağlamak ve kullanıcıların gizlilik haklarını korumak amacıyla hazırlanmıştır. CNIL'in rehberinde, kullanıcıların mobil uygulamalara hangi verilere ve fonksiyonlara erişim izni verebileceği üzerine önemli bilgiler yer almaktadır.

CNIL, mobil uygulamaların gereksiz veri taleplerinden kaçınmasını ve her izin talebinin belirli bir hukuki temele dayanmasını sağlamayı öneriyor. İzin taleplerinin serbestçe verilmiş, belirli, bilgilendirilmiş ve açık olması gerektiğini vurgulayan CNIL, kullanıcıların yalnızca gerekli verileri paylaşmalarını sağlamak için uygulamaların veri minimizasyonu ilkesine uygun davranmasını önermektedir. Özellikle, uygulamalar yalnızca hizmetin işleyişi için gerekli olan verilere erişim talep etmelidir. İşletim sistemi sağlayıcılarının izin sistemlerini, izinlerin kapsamını ayrıntılı bir şekilde belirleyecek şekilde tasarlaması gerektiği belirtilmiştir. Ayrıca, geliştiricilerin kullanıcıların gereksiz veri taleplerini fark etmelerini sağlamak için uygulamalarında şeffaflık ve basitlik sunması gerektiği vurgulanmıştır. İzin talepleri, kullanıcı deneyimini bozmadan, anlaşılır bir şekilde ve doğru bağlamda sunulmalıdır.

CNIL, teknik izinler ve kullanıcı rızasının birlikte kullanılmasının gerektiğini belirtmekte ve bu iki sürecin kullanıcıyı karmaşaya sürüklememesi için dikkat edilmesi gerektiğini vurgulamaktadır. Ayrıca, izin taleplerinin zamanlaması, izinlerin süresi ve hangi verilere erişileceği konusunda kullanıcıya net bilgiler verilmelidir.

Sonuç olarak, CNIL'in önerileri, mobil uygulama geliştiricilerinin ve veri sorumlularının, GDPR'ye uygun bir şekilde kullanıcı verilerini toplarken gizliliği sağlamalarına yardımcı olacak rehberlik sunmaktadır.

İlgili içeriğe buradan ulaşabilirsiniz.

31 Ocak 2025 I Fransa'nın veri koruma otoritesi CNIL, kuruluşların veri transferi etki değerlendirmeleri (TIA) yapmasına yardımcı olmak için güncellenmiş bir rehber yayımladı. (1/2)

Fransa'nın veri koruma otoritesi CNIL, kuruluşların veri transferi etki değerlendirmeleri (Transfer Impact Assessment - TIA) yapmasına yardımcı olmak amacıyla güncellenmiş bir rehber yayımlamıştır.

Bu rehber, Avrupa Ekonomik Alanı dışına kişisel veri transferi gerçekleştiren veri sorumluları ve veri işleyenler için GDPR'nin 46. maddesine dayalı transfer araçlarını kullanırken rehberlik sunmayı amaçlamaktadır. Rehber, Schrems II kararından sonra ortaya çıkan gerekliliklere uyum sağlamak ve veri ihracatçılarının üçüncü ülkelere veri transferinde yeterli koruma seviyesini değerlendirmelerine destek olmak için tasarlanmıştır.

Veri Koruma I Avrupa Birliği I Birleşik Krallık

31 Ocak 2025 I Fransa'nın veri koruma otoritesi CNIL, kuruluşların veri transferi etki değerlendirmeleri (TIA) yapmasına yardımcı olmak için güncellenmiş bir rehber yayımladı. (2/2)

Rehber, veri transferi etki değerlendirmeleri sürecini altı temel adımda düzenlemektedir: (1) Transferin bilinmesi, (2) Kullanılan transfer aracının belgelenmesi ,(3) Hedef ülkedeki mevzuat ve uygulamaların transfer aracının etkinliğiyle birlikte değerlendirilmesi, (4) Ek koruma önlemlerinin belirlenmesi ve benimsenmesi, (5) Bu önlemlerin ve gerekli prosedürlerin uygulanması, (6) Veri koruma seviyesinin düzenli aralıklarla yeniden değerlendirilmesi ve olası gelişmelerin izlenmesi. CNIL, bu adımların her biri için kuruluşlara pratik bir metodoloji ve doldurulabilir tablolar sunarak transferin hukuki ve pratik risklerini analiz etmelerine olanak tanımaktadır.

Rehber, özellikle veri ithalatçısının iş birliğinin önemini vurgulamakta ve GDPR Madde 28 kapsamında veri işleyenlerin veri sorumlularına somut bilgiler sağlama yükümlülüğünü öne çıkarmaktadır.

İlgili rehbere buradan ulaşabilirsiniz.

30 Ocak 2025 I İtalya Veri Koruma otoritesi Deepseek'e erişim engeli getirdi.

İtalya Veri Koruma Otoritesi (Garante per la Protezione dei Dati Personali - GPDP), Çin merkezli yapay zekâ uygulaması DeepSeek'e 30 Ocak 2025 tarihinde erişim engeli getirmiştir. Bu karar, DeepSeek'in kişisel verilerin toplanması, işlenmesi ve saklanmasına dair İtalyan yetkililerin bilgi taleplerine verdiği yanıtın "tamamen yetersiz" bulunması üzerine alınmıştır. GPDP, DeepSeek'ten hangi kişisel verilerin, hangi kaynaklardan, hangi amaçlarla ve hangi yasal dayanakla toplandığını, ayrıca bu verilerin Çin'de depolanıp depolanmadığını sormuş, ancak şirketin açıklamaları tatmin edici bulunmamıştır. Bunun sonucunda, 29 Ocak 2025'ten itibaren DeepSeek İtalya'daki Apple ve Google uygulama mağazalarından indirilemez hale gelmiş ve ülkede erişime kapatılmıştır.

İlgili içeriğe buradan ulaşabilirsiniz.

5 Şubat 2025 I Birleşik Krallık'ın veri koruma otoritesi ICO, istihdam kayıtlarının mevzuata uygun işlenmesi hakkında rehber yayımladı. (1/2)

Birleşik Krallık Veri Koruma Otoritesi (ICO), işverenlerin istihdam kayıtlarını UK GDPR ve Veri Koruma Yasası 2018 (DPA 2018) ile uyumlu bir şekilde işleyebilmesi için kapsamlı bir rehber yayımlamıştır. Bu rehber, işverenlerin çalışanlarının kişisel verilerini toplama, saklama ve kullanma süreçlerinde veri koruma ilkelerine uyması gerektiğini vurgulamaktadır. İşverenlerin, hangi verileri neden topladıklarını açıkça tanımlaması ve bu verileri işlemek için UK GDPR Madde 6'da yer alan hukuki temellerden birine dayanması gerekmektedir. Rehber, işveren ile çalışan ilişkisindeki güç dengesizliği nedeniyle rızanın genellikle geçerli bir hukuki temel olarak kullanılamayacağını özellikle belirtmektedir. Özel nitelikli veri işleniyor ise UK GDPR Madde 9 uyarınca ek bir koşulun karşılanması gerektiği ve bu tür verilerin daha sıkı koruma önlemleriyle işlenmesi gerektiği açıklanmaktadır. Ayrıca, işverenlerin veri minimizasyonu ilkesine uyması, yalnızca gerekli olan verileri toplaması ve bu verileri yalnızca ihtiyaç duyulan süre boyunca saklaması gerektiği ifade edilmekle beraber bu amaçla bir saklama politikası oluşturulması önerilmektedir.

Veri Koruma I Avrupa Birliği I Birleşik Krallık

5 Şubat 2025 I Birleşik Krallık'ın veri koruma otoritesi ICO, istihdam kayıtlarının mevzuata uygun işlenmesi hakkında rehber yayımladı. (2/2)

Rehber, istihdam kayıtlarının pratik yönetiminde işverenlerin karşılaşabileceği çeşitli senaryoları da ele almaktadır. Örneğin, işverenlerin çalışan verilerini bordro şirketleri, sigorta sağlayıcıları veya yeni işverenler gibi üçüncü taraflarla paylaşması gerektiğinde, bu paylaşımın amacı açıkça belirtilmeli ve çalışanlar bilgilendirilmelidir. TUPE (Transfer of Undertakings- Protection of Employment, İşletmelerin Devri ve Çalışanların Haklarının Korunması) düzenlemeleri kapsamında, bir işin devri sırasında çalışan verilerinin nasıl paylaşılacağı ve korunacağı konusunda rehberlik sunmaktadır. Rehber; işverenlerin eşitlik izleme, emeklilik planları için veri işleme veya dış kaynak kullanımı gibi spesifik durumlarda da veri koruma kurallarına uyması gerektiğini detaylandırmaktadır. Bu süreçlerde, işverenlerin çalışanlara yönelik şeffaflık yükümlülüklerini yerine getirmesi, hangi verilerin toplandığını, nasıl kullanıldığını ve kimlerle paylaşıldığını açıkça bildirmesi gerektiği vurgulanmaktadır.

ICO'nun bu rehberi, işverenlerin veri koruma yükümlülükleriyle iş operasyonlarının ihtiyaçları arasında bir denge kurmasını sağlamayı hedeflemektedir. Çalışanların gizlilik haklarının korunmasının yanı sıra, işverenlerin yasal ve operasyonel gereklilikleri yerine getirebilmesi için pratik çözümler önerilmektedir. Rehber, işverenlerin veri ihlallerini önlemek ve çalışanlardan gelen veri taleplerine doğru şekilde yanıt vermek için proaktif bir yaklaşım benimsemesi gerektiğini savunmaktadır. Ayrıca, işverenlerin veri işleme faaliyetlerini düzenli olarak gözden geçirmesi ve gerektiğinde bir Veri Koruma Etki Değerlendirmesi (DPIA) yapması gerektiği belirtilmekle beraber, özellikle yüksek riskli veri işleme faaliyetleri için kritik bir adım olarak görülmektedir.

İgili rehbere buradan ulaşabilirsiniz.

7 Şubat 2025 I İngiltere hükümet yetkililerinin Apple'dan, 'dünya çapındaki herhangi bir Apple kullanıcısının buluta yüklediği tüm içeriğe' arka kapı erişimi sağlamasını talep ettiği belirtildi. (1/2)

Birleşik Krallık yetkililerinin, Apple'dan dünya çapındaki tüm Apple kullanıcılarının buluta yüklediği içeriklere arka kapı erişimi sağlamasını talep ettiği yönündeki iddia, 2025 yılının başında veri gizliliği ve ulusal güvenlik alanında önemli bir tartışma konusu haline gelmiştir.

Bu talep, Birleşik Krallık İçişleri Bakanlığı tarafından Ocak 2025'te Apple'a iletilen bir Teknik Yetkinlik Bildirimi (Technical Capability Notice) yoluyla resmi olarak sunulmuştur. Bildirim, Apple'ın iCloud hizmetinde uyguladığı uçtan uca şifreleme sistemini, özellikle Gelişmiş Veri Koruması (veri güvenliğini artırmak için kullanılan bir teknoloji, Advanced Data Protection - ADP) özelliğini hedef almaktadır. ADP, kullanıcıların iCloud yedeklemelerini yalnızca kendilerinin erişebileceği şekilde şifreleyerek, Apple dahil hiçbir üçüncü tarafın bu verilere ulaşmasını engellemektedir. İngiltere'nin talebi, bu şifreleme sistemine bir arka kapı entegre edilmesini ve dünya genelindeki tüm kullanıcı verilerine erişim yetkisi tanınmasını kapsamakta olup, bu durum, demokratik ülkeler arasında benzeri görülmemiş bir müdahale olarak değerlendirilmektedir.

Veri Koruma I Avrupa Birliği I Birleşik Krallık

7 Şubat 2025 I İngiltere hükümet yetkililerinin Apple'dan, 'dünya çapındaki herhangi bir Apple kullanıcısının buluta yüklediği tüm içeriğe' arka kapı erişimi sağlamasını talep ettiği belirtildi. (2/2)

Birleşik Krallık hükümeti, söz konusu talebin ulusal güvenlik ve ciddi suçlarla mücadele gerekliliklerinden kaynaklandığını öne sürmektedir. Özellikle çocuk istismarı ve terörizm gibi suçların önlenmesi amacıyla şifreli verilere erişim ihtiyacı belirtilmişse de talep belirli bir hesaba yönelik sınırlı bir erişimle kısıtlı kalmamakta ve bunun yerine, tüm Apple kullanıcılarının iCloud verilerine genel bir erişim yetkisi öngörülmektedir. Apple, bu talebe kesin bir şekilde karşı çıkarak, bireylerin gizlilik haklarını temel bir ilke olarak gördüğünü ve kullanıcılarına sunduğu güvenlik taahhütlerinden vazgeçmeyeceğini açıklamıştır. Şirket, böyle bir arka kapının yalnızca Birleşik Krallık için değil, küresel ölçekte tüm kullanıcıların veri güvenliğini tehlikeye atacağını ifade etmiştir. Apple, bu talebe uymak yerine, Şubat 2025 itibarıyla Birleşik Krallık'ta ADP özelliğini yeni kullanıcılar için devre dışı bırakmış ve mevcut kullanıcılar için de aşamalı olarak kaldırma sürecini başlatmıştır.

İlgili içeriğe buradan ulaşabilirsiniz.

10 Şubat 2025 I Birleşik Krallık veri koruma otoritesi ICO, Lordlar Kamarası'ndan geçen Veri (Kullanım ve Erişim) (DUA) Tasarısı'na yönelik güncellenmiş görüşünü yayımladı.

Birleşik Krallık Veri Koruma Otoritesi (ICO), Lordlar Kamarası'ndan geçen Veri (Kullanım ve Erişim) (DUA) Tasarısı'na yönelik güncellenmiş görüşünü yayımlayarak tasarının veri koruma rejiminde önerdiği değişikliklere kapsamlı bir değerlendirme sunmaktadır. ICO, tasarının bilimsel araştırma tanımını netleştiren ve genişleten hükümlerini desteklemektedir. Tasarı, kişisel verilerin bilimsel araştırma amacıyla işlenmesini "kamu yararı doğrultusunda, makul bir şekilde bilimsel olarak tanımlanabilecek herhangi bir araştırma" olarak sınırlamakta ve bu faaliyetlerin fonlama türüne bakılmaksızın geçerli olduğunu ifade etmektedir. ICO, bu değişikliğin araştırmacılara daha fazla açıklık ve esneklik sağlarken, bireylerin korunmasını sürdüreceğini düşünmektedir. Ayrıca, "kamu yararı" kavramının yorumlanmasına yönelik rehber yayımlamayı taahhüt etmektedir.

ICO'nun görüşünde, çocukların verilerine yönelik geliştirilmiş korumalar da yer almaktadır. Tasarı, çocukların kişisel verilerinin özel koruma gerektirdiğine vurgu yaparak, veri işleyenlerin bu konuda daha fazla sorumluluk almasını öngörmektedir. Yapılan değişiklikler, özellikle çevrim içi hizmetlerde çocukların verilerinin işlenmesi sırasında "yüksek koruma önlemleri" alınmasını zorunlu kılmaktadır. ICO, bu ek korumaların çocukların verilerine yönelik düzenlemelerde yüksek bir yasal standart oluşturduğu izlenimi yaratmaması gerektiğini vurgulamaktadır.

Son olarak, ICO yapay zekâ ve otomatik karar alma süreçlerine ilişkin tasarının getirdiği yeni kuralları da desteklemektedir. Tasarı, otomatik karar alma süreçlerinin belirli koruma önlemleriyle yasal temele dayandırılabileceğini öngörmekte ve bu alanda esneklik sağlamaktadır. Özellikle, özel kategori verilerin işlenmesi durumunda ek koruma önlemleri ve "anlamlı insan müdahalesi" gibi unsurların önemine dikkat çekilmektedir.

İlgili içeriğe buradan ulaşabilirsiniz.

Veri Koruma I Avrupa Birliği I Birleşik Krallık

11 Şubat 2025 I Avrupa Veri Koruma Kurulu (EDPB), çocuklara yönelik yaş güvencesi hakkında bir görüş bir kabul etti.

Avrupa Veri Koruma Kurulu (EDPB), çocukların çevrim içi güvenliğini sağlamak ve kişisel verilerinin korunmasını temin etmek amacıyla "yaş güvencesi" (age assurance) ile ilgili bir görüş yayımlamıştır. Bu görüş, dijital ortamda çocukların yaşını doğrularken kişisel verilerin nasıl işlenmesi gerektiğine dair rehberlik sunmaktadır. EDPB, çocukların kişisel verilerinin yalnızca gerekli olduğunda ve doğru şekilde işlenmesi gerektiğini vurgulamaktadır. Bu kapsamda, yaş doğrulama işlemi yapılırken yalnızca gerekli verilerin toplanması gerektiği belirtilmektedir. Ayrıca, çocuklar ve ebeveynlerinin hangi verilerin toplandığı ve bu verilerin nasıl kullanılacağı konusunda açık bir şekilde bilgilendirilmesi ve verilerin güçlü güvenlik önlemleriyle korunması gerektiği ile çocukların kişisel verileri üzerinde ebeveynlerin kontrol sahibi olmasının önemine dikkat çekilmektedir. 13 yaşından küçük çocuklar için veri işleme, ebeveyn onayıyla yapılmalıdır. EDPB'nin bu görüşü, dijital platformların ve hizmet sağlayıcılarının yaş doğrulama sistemlerini doğru bir şekilde uygulamaları gerektiğini hatırlatarak, çocukların internet ortamında daha güvenli bir şekilde var olmalarını ve kişisel verilerinin korunmasını sağlamayı hedeflemektedir.

İlgili içeriğe buradan ulaşabilirsiniz.

13 Şubat 2025 I Bir ABAD kararında, veri koruma otoriteleri ve mahkemelerin para cezası miktarlarını belirlerken veri sorumlusunun bir teşebbüsün parçası olup olmadığını dikkate almaları gerektiği belirtilmiştir.

Avrupa Birliği Adalet Divanı'nın (ABAD) Case C-383/23 ILVA A/S kararında, veri koruma otoritelerinin ve mahkemelerin, GDPR kapsamında para cezası miktarlarını belirlerken veri sorumlusunun bir teşebbüsün parçası olup olmadığını dikkate alması gerektiği hükme bağlanmıştır. Bu karar, Danimarka'da ILVA A/S adlı bir şirkete veri koruma otoritesinin uyguladığı cezada, şirketin bağlı olduğu Lars Larsen Group'un toplam cirosunun esas alınıp alınmaması gerektiği sorusunu ele almaktadır. ABAD, para cezalarının azami miktarının, veri sorumlusunun kendi cirosuna değil, teşebbüsün (örneğin, şirketler grubunun) dünya çapındaki yıllık cirosuna dayanması gerektiğini vurgulayarak, cezaların caydırıcı ve orantılı olmasını sağlamayı amaçlamıştır. Bu yaklaşım, bir yan kuruluşun küçük cirosuna rağmen, daha büyük bir ekonomik birimin parçasıysa, cezaların bu birimin gücünü yansıtacak şekilde hesaplanması gerektiğini ortaya koymaktadır.

Kararda, teşebbüs kavramının Avrupa Birliği rekabet hukuku (TFEU Madde 101 ve 102) çerçevesinde tanımlandığına da dikkat çekiliyor. Case C-383/23 ILVA A/S, bir ana şirketin yan kuruluşları üzerinde belirleyici kontrolü varsa, tüm grubun tek bir ekonomik birim olarak değerlendirilebileceğini netleştiriyor. Bu, GDPR'nin 83. maddesine dayanan bir yorumla, veri koruma ihlallerinde cezaların yalnızca ihlali gerçekleştiren kuruluşun finansal kapasitesine odaklanmaması gerektiğini ifade etmektedir. Büyük çok uluslu şirketler için daha yüksek cezalar anlamına gelen bu hüküm, veri koruma kurallarına uyumu teşvik etmeyi hedefler ve uygulamada önemli bir emsal oluşturmaktadır.

Karar, 2025 itibarıyla veri koruma otoritelerine, cezaları hesaplarken ekonomik gerçeklikleri daha geniş bir perspektiften ele alma zorunluluğu getirerek, veri koruma rejiminde tutarlılık ve etkinlik sağlamayı amaçlamaktadır.

İlgili içeriğe buradan ulaşabilirsiniz.

Veri Koruma I Avrupa Birliği I Birleşik Krallık

18 Şubat 2025 I İsveç veri koruma otoritesi, Veri Koruma Etki Değerlendirmesi (DPIA) yürütme konusunda bir rehber yayımlamıştır.

İsveç Veri Koruma Otoritesi (IMY) tarafından yayımlanan Veri Koruma Etki Değerlendirmesi (DPIA) rehberi, GDPR Madde 35 kapsamında veri sorumlularına yüksek riskli veri işleme faaliyetlerini yönetmek için kapsamlı bir yol haritası sunmaktadır. Rehber, DPIA gerekliliğinin değerlendirilmesiyle başlayarak veri sorumlularının hangi durumlarda bu analizi yapması gerektiğini açıkça ortaya koymaktadır. İşleme faaliyetlerinin sistematik bir şekilde tanımlanması gerektiği belirtmekte ve bu doğrultuda işleme amacını, kapsamını ve bağlamını içermektedir. Ayrıca, hukuki analiz yapılarak veri işlemenin GDPR'daki meşru dayanaklarının incelenmesi gerektiği vurgulanmaktadır.

Rehberin bir diğer temel unsuru, risk tanımlama ve azaltma süreçlerine odaklanmasıdır. DPIA'nın, veri ihlali, ayrımcılık veya mahremiyet kaybı gibi potansiyel riskleri belirlemesi ve bu risklerin niteliğini, kaynağını ve etkisini değerlendirmesi gerektiği ifade edilmektedir. Riskler belirlendikten sonra, bu tehditleri en aza indirmek için şifreleme, erişim kontrolleri gibi teknik ve organizasyonel önlemlerin uygulanması önerilmektedir. IMY, bu süreçlerin paydaşlarla iş birliği içinde yürütülmesini ve gerektiğinde otoriteyle ön istişare yapılmasını tavsiye etmektedir.

Bu rehber, İsveç'teki veri sorumlularına pratik ve uygulanabilir bir çerçeve sunarak GDPR uyumluluğunu güçlendirmeyi hedeflemektedir. Yüksek riskli veri işleme faaliyetlerinin yönetimini sadeleştiren rehber, veri koruma etiği ve hesap verebilirlik ilkelerini desteklemekle birlikte veri sorumlularının risk yönetimi süreçlerini yapılandırmasına olanak tanıyarak bireylerin hak ve özgürlüklerini korumayı önceliklendirerek veri koruma rejiminde tutarlılık ve etkinlik sağlamayı amaçlamaktadır.

İlgili rehbere buradan ulaşabilirsiniz.

26 Şubat 2025 I Avrupa Parlamentosu Araştırma Servisi (EPRS), AB Yapay Zekâ Yasası (AI Act) ile GDPR arasındaki etkileşimin ve algoritmik ayrımcılığın bu düzenlemeler çerçevesinde nasıl ele alındığının incelendiği bir çalışma yayımlamıştır. (1/2)

EPRS'nin çalışması, 2024 yılı Ağustos ayında yürürlüğe giren AI Act'in, GDPR ile olan ilişkisini ve algoritmik ayrımcılıkla nasıl başa çıkılacağını anlamaya yönelik bir açıklama sunmaktadır. AI Act, güvenilir, sürdürülebilir ve insan odaklı yapay zekâ (YZ) kullanımını teşvik etmeyi amaçlarken, bireylerin temel haklarını, özellikle veri koruma haklarını koruma önceliğine sahiptir. Bu bağlamda, AI Act, "yüksek riskli YZ sistemlerinde" ayrımcılık ve önyargıları azaltmayı hedefler. AI Act'in 10(5) maddesi, önyargıların izlenmesi, tespiti ve düzeltilmesi amacıyla, özel kategori kişisel verilerinin işlenmesine izin vermekte, ancak bu işleme sadece temel haklar gözetilerek yapılmalıdır.

EPRS, algoritmik ayrımcılığın farklı sektörlerde nasıl sorunlar yaratabileceğine dair örnekler sunmaktadır. Örneğin, üretken YZ sistemleri nefret söylemi üretebilir ve temel hakları tehdit edebilir; bu tür sistemler genellikle yüksek riskli sayılmasa da, hak ihlalleri yaratanlar AI Act kapsamında yüksek riskli olarak değerlendirilebilir. Otonom araçlar, deri rengine göre yayaları farklı doğrulukla algılayarak ayrımcılığa yol açabilir. Benzer şekilde, işe alım ve bankacılık sektörlerinde kullanılan YZ sistemleri cinsiyet, sağlık durumu, ikamet yeri veya etnik köken gibi faktörlere dayalı önyargıları barındırabilir.

Veri Koruma I Avrupa Birliği I Birleşik Krallık

26 Şubat 2025 I Avrupa Parlamentosu Araştırma Servisi (EPRS), AB Yapay Zekâ Yasası (AI Act) ile GDPR arasındaki etkileşimin ve algoritmik ayrımcılığın bu düzenlemeler çerçevesinde nasıl ele alındığının incelendiği bir çalışma yayımlamıştır. (2/2)

AI Act, bu tür ayrımcılığın azaltılması için özel kategori verilerin işlenmesine izin verirken, GDPR'ın daha katı veri koruma kuralları bu süreci sınırlayabilir. EPRS, bu iki düzenleme arasında çelişkiler olduğuna dikkat çekmekte ve AI Act'in algoritmik ayrımcılığı önleme hedefinin GDPR'ın katı veri koruma kuralları ile nasıl dengeleyeceği konusunda belirsizlikler bulunduğunu vurgulamaktadır. Bu durum, YZ'nin giderek daha yaygın bir şekilde kullanılmasıyla birlikte, bireylerin haklarının korunması ve teknolojik ilerlemenin desteklenmesi arasında bir gerilim yaratmaktadır.

İlgili içeriğe buradan ulaşabilirsiniz.

27 Şubat 2025 I Avrupa Birliği Adalet Divanı'nın (ABAD) C-203/22 sayılı Kararında, otomatik yollarla gerçekleştirilen kredi değerlendirmesi kapsamında, ilgili kişinin kendisi hakkında alınan kararın nasıl verildiğine dair açıklama talep etme hakkına sahip olduğu ve bu açıklamanın, ilgili kişinin kararı anlamasına ve itiraz etmesine imkân tanıyacak nitelikte olması gerektiğine hükmedilmiştir.

ABAD'ın C-203/22 sayılı kararı, otomatik kredi değerlendirme süreçlerinde veri sahiplerinin haklarını ele alan önemli bir karar olan olayda Avusturya'da bir mobil telefon operatörü, Dun & Bradstreet Austria'nın otomatik değerlendirmesi sonucu bir müşterinin kredi başvurusunu reddetmiştir. Müşteri, kararın nasıl alındığını anlamak için açıklama talep etmiş, ancak şirket yalnızca genel bilgi sunmuş ve kararın mantığını yeterince açıklamamıştır. Bu durum, Avusturya mahkemesi tarafından GDPR ihlali olarak değerlendirilmiş ve ABAD'a başvurulmuştur.

ABAD, kararında veri sorumlusunun, otomatik olarak alınan bir kararın nasıl verildiğine dair veri sahibine anlamlı açıklama yapma yükümlülüğü olduğunu belirtmektedir. Açıklama, veri sahibinin hangi verilerinin kullanıldığını ve bu verilerin karar süreçlerinde nasıl etkili olduğunu anlamasına yardımcı olmaktadır. Ayrıca açıklamanın şeffaf, açık ve anlaşılır olması gerektiği vurgulanmaktadır. Yalnızca algoritmanın paylaşılması yeterli bulunmamaktadır. ABAD ayrıca, veri sorumlusunun ticari sırlarını gerekçe göstererek bu bilgileri vermemesi durumunda, ilgili bilgilerin denetim otoritesine veya mahkemeye sunulması gerektiğini belirtmektedir. Bu otorite veya mahkeme, veri sahibinin erişim hakkı ile ticari sırların korunması arasındaki dengeyi belirleyecek kararlar almaktadır.

Sonuç olarak, ABAD, GDPR kapsamında veri sahiplerinin haklarını güçlendirmekte ve otomatik karar alma süreçlerinde şeffaflık ve hesap verebilirlik ilkesine vurgu yapmaktadır.

İlgili içeriğe buradan ulaşabilirsiniz.

Veri Koruma I Avrupa Birliği I Birleşik Krallık

5 Mart 2025 I Avrupa Veri Koruma Kurulu (EDPB) tarafından, GDPR'ın silme hakkı ile ilgili koordineli uygulama çalışması başlatılmıştır.

Avrupa Veri Koruma Kurulu (EDPB), GDPR'ın 17. maddesi kapsamında yer alan silme hakkı ile ilgili bir koordineli uygulama çalışması (Coordinated Enforcement Framework - CEF) başlatmıştır. Bu çalışma, EDPB'nin 2024-2027 Stratejisi çerçevesinde, veri koruma otoriteleri arasında iş birliğini ve tutarlılığı artırmayı amaçlayan dördüncü CEF eylemi olarak 5 Mart 2025 tarihinde duyurulmuştur. Silme hakkı, bireylerin en sık kullandığı veri koruma haklarından biri olup, aynı zamanda veri koruma otoritelerine en çok şikayet edilen konulardan biridir. Bu nedenle, EDPB, 2025 yılı boyunca bu hakkın veri sorumluları tarafından pratikte nasıl uygulandığını değerlendirmeyi hedeflemektedir.

Koordineli uygulama çalışması, 32 Avrupa veri koruma otoritesinin katılımıyla gerçekleştirilecektir. Katılımcı otoriteler, farklı sektörlerden veri sorumlularıyla iletişime geçerek, silme hakkının uygulanışını inceleyeceklerdir. Çalışmanın amacı, veri sorumlularının silme taleplerine nasıl yanıt verdiği, bu hakkın uygulanmasında hangi süreçlerin izlendiği ve GDPR'da belirtilen koşul ve istisnaların nasıl ele alındığını değerlendirmektir. Bulguların, ulusal düzeydeki uygulamaların toplu bir şekilde değerlendirilmesiyle EDPB tarafından bir rapor haline getirilerek 2026 başında yayımlanması planlanmaktadır.

İlgili içeriğe buradan ulaşabilirsiniz.

5 Mart 2025 I Avrupa Sağlık Veri Alanı'na ilişkin 2025/327 sayılı Tüzük, AB Resmi Gazetesi'nde yayımlandı.

Avrupa Sağlık Veri Alanı'nı (EHDS) kurmayı amaçlayan 2025/327 sayılı Tüzük, bireylerin kişisel sağlık verilerine erişim ve kontrol sağlamayı amaçlamaktadır. 5 Mart 2025 tarihinde AB Resmi Gazetesi'nde yayımlanan bu tüzük, Avrupa Birliği İşleyiş Antlaşması'na dayanarak, sağlık verilerinin güvenli bir şekilde paylaşılmasını kolaylaştırmayı hedeflemektedir. Tüzük, Avrupa genelinde kişisel sağlık verilerinin ortak bir elektronik formatta (European electronic health record exchange format) kullanılmasını sağlayarak, sağlık hizmetleri, araştırma, inovasyon ve sağlık tehditlerine hazırlık gibi toplumsal fayda sağlayan amaçlarla bu verilerin paylaşılmasına olanak tanımaktadır.

Tüzük, bireylerin sağlık verilerine erişim haklarını güçlendirirken, verilerin güvenli ve etik bir şekilde işlenmesini garanti etmektedir. Bireyler, tıbbi geçmiş, teşhisler, reçeteler gibi kişisel sağlık verilerine kolayca erişebilmekte ve bu verileri seçtikleri sağlık uzmanlarıyla paylaşabilmektedir. Ayrıca, bu veriler sosyal güvenlik hizmetlerine aktarılabilmektedir. Üye devletler, bireylerin tamamen vazgeçme hakkını düzenleyebilmektedir. Ayrıca tüzük, sağlık verilerinin ikincil kullanımını da düzenler. Örneğin, araştırma veya politika yapımında kullanılacak veriler, Sağlık Veri Erişim Kurumları aracılığıyla sağlanacaktır. Bu süreçte bireyler, ikincil kullanıma onay vermek zorunda değildir ve bu veriler "bulunabilir, erişilebilir, birlikte çalışabilir ve yeniden kullanılabilir" (FAIR) ilkelere uygun olarak işlenilebilecektir.

İlgil Tüzük'e buradan ulaşabilirsiniz.

Veri Koruma I Küresel

14 Şubat 2025 I Çin Siber Uzay İdaresi (CAC), 1 Mayıs 2025'te yürürlüğe girecek olan Kişisel Veri Koruma Uyumluluk Denetimi Yönetim Tedbirlerini onayladı. Tedbirler, 10 milyondan fazla kişinin verilerini işleyen kuruluşların iki yılda bir denetim yapması gibi uyumluluk denetimleri yapılması gibi zorunluluklar içeriyor.

Çin Siber Uzay İdaresi (CAC), kişisel veri korumasını güçlendirmek amacıyla "Kişisel Veri Koruma Uyumluluk Denetimi Yönetim Tedbirleri"ni onayladı. Bu tedbirler, 1 Mayıs 2025 tarihinde yürürlüğe girecek ve büyük veri işleyen kuruluşların PIPL (Kişisel Bilgi Koruma Yasası) ve DSL (Veri Güvenliği Yasası) ile uyumlu olup olmadığını denetlemeyi amaçlamaktadır. Özellikle 10 milyon ve üzeri kişisel veri işleyen kuruluşlar, her iki yılda bir zorunlu uyumluluk denetimi yapacaktır. Bu denetimler, veri toplama, işleme ve güvenlik önlemleri gibi süreçleri değerlendirecektir. Denetim sonuçları CAC'a bildirilecek ve eksikliklerin giderilmesi için bir zaman çizelgesi sunulacaktır. Tedbirler, veri kötüye kullanımını önlemeyi, güvenlik risklerini azaltmayı ve bireylerin veri koruma haklarını güçlendirmeyi hedeflemektedir. Bu kapsamda uyum sağlamayan kuruluşlar, cezalarla karşılaşabilecektir.

İlgili içeriğe buradan ulaşabilirsiniz.

17 Şubat 2025 I Güney Kore veri koruma otoritesi, yapay zekâ modeli DeepSeek hizmetlerini 15 Şubat 2025 itibarıyla geçici olarak askıya aldı.

Güney Kore'nin veri koruma otoritesi, Kişisel Bilgileri Koruma Komisyonu (Personal Information Protection Commission - PIPC), Çin merkezli yapay zekâ modeli DeepSeek'in hizmetlerini 15 Şubat 2025 itibarıyla geçici olarak askıya almıştır. Bu karar, DeepSeek'in kişisel veri toplama ve işleme uygulamalarına ilişkin ciddi endişeler nedeniyle alınmıştır. PIPC, DeepSeek'in Güney Koreli kullanıcıların verilerini nasıl topladığı, işlediği ve bu verilerin Çin merkezli sunucularda depolanıp depolanmadığı konusunda şeffaf bilgi sağlamadığını tespit etmiştir. Ayrıca, DeepSeek'in veri güvenliği politikalarının Güney Kore'nin Kişisel Bilgi Koruma Yasası (Personal Information Protection Act - PIPA) ile uyumlu olup olmadığına dair bir soruşturma başlatılmıştır.

Soruşturmanın temel nedenlerinden biri, DeepSeek'in kullanıcı verilerini ByteDance (TikTok'un ana şirketi) gibi üçüncü taraflarla paylaştığına dair iddialardır. Güney Kore Ulusal İstihbarat Teşkilatı (NIS) ve PIPC, DeepSeek'in aşırı miktarda kişisel bilgi topladığını ve bu verilerin Çin hükümetinin erişimine açık olabileceği riskini vurgulamıştır. Bu durum, ulusal güvenlik ve bireylerin gizlilik hakları açısından bir tehdit olarak değerlendirilmiştir. 15 Şubat 2025'te yürürlüğe giren askıya alma kararıyla DeepSeek'in uygulamaları yerel uygulama mağazalarından kaldırılmış ve web erişimi engellenmiştir; ancak, uygulamayı daha önce indirmiş olan kullanıcılar için kullanım devam edebilmektedir. PIPC, DeepSeek'in Güney Kore yasalarına uyum sağlayacak düzenlemeler yapana kadar bu yasağın süreceğini ve şirketten resmi bir yanıt beklendiğini belirtmiştir.

İlgili içeriğe buradan ulaşabilirsiniz.

Veri Koruma I Küresel

21 Şubat 2025 I İngiltere'nin Apple'a bir şifreleme arka kapısı inşa etmesini emretmesinin ardından ABD Kongresi, ABD teknoloji şirketlerinin herhangi bir ülkeye bu tür arka kapılar sağlamasını yasaklayan bir yasa çıkardı.

İngiltere'nin Apple'a, kullanıcıların iCloud verilerine erişim için bir şifreleme arka kapısı inşa etmesini emretmesi, 2025'in başında uluslararası bir tartışma yaratmıştır. Apple bu talebe karşı çıkarak, böyle bir arka kapının yalnızca İngiltere için değil, küresel çapta tüm kullanıcıların gizliliğini ve güvenliğini tehlikeye atacağını savunmuştur. Şirket, bu talebe uymaktansa ADP hizmetini Birleşik Krallık'ta devre dışı bırakma yoluna gitmiş ve Şubat 2025'te bu özelliği yeni kullanıcılar için kapatmıştır.

Bu kapsamda, İngiltere'nin talebinin Amerikan vatandaşlarının verilerini de riske atabileceği endişesiyle bir yasa tasarısı hazırlanmıştır. 14 Mart 2025'te Kongre tarafından kabul edilen bu yasa, ABD teknoloji şirketlerinin herhangi bir yabancı ülkeye şifreleme arka kapıları sağlamasını yasaklamıştır. "Amerikan Teknoloji Güvenlik Yasası" (American Tech Security Act) olarak adlandırılan bu düzenleme, ABD merkezli şirketlerin yabancı hükümetlerin taleplerine uyarak ürünlerinde güvenlik zayıflıkları oluşturmasını engellemeyi amaçlamaktadır. Yasa, aynı zamanda 2018 tarihli CLOUD Yasası'nı (Clarifying Lawful Overseas Use of Data Act) güncelleyerek, uluslararası veri paylaşım anlaşmalarında Kongre'nin denetimini artırmakta ve ABD firmalarının bu tür taleplere karşı federal mahkemelerde itiraz hakkını güçlendirmektedir.

İlgili içeriğe buradan ulaşabilirsiniz.

23 Şubat 2025 I Japonya veri koruma otoritesi, şirketlerin yapay zekâ sistemlerini eğitmek için kişisel verilerin kullanımına dair önceden izin alma gerekliliğini kaldırmayı düşündüğünü açıkladı.

Japonya Kişisel Bilgi Koruma Komisyonu (PPC), 2025 başında, yapay zekâ (YZ) sistemlerini eğitmek için kişisel verilerin kullanılmasında önceden izin alma gerekliliğini kaldırmayı değerlendirdiğini açıkladı. Bu öneri, Japonya'nın Kişisel Bilgi Koruma Yasası (APPI) çerçevesinde yapılan düzenlemelerin gözden geçirilmesi sürecinin bir parçası olarak sunuldu. PPC, bu değişikliğin, YZ teknolojilerinde inovasyonu teşvik etmeyi ve küresel rekabeti artırmayı hedeflediğini belirtilmiştir. Öneri, kişisel verilerin YZ eğitimi için "meşru menfaat" temelinde işlenmesini sağlayacak ancak şeffaflık, veri minimizasyonu ve bireylerin haklarını koruma gibi ek yükümlülükler getirecektir. Ayrıca, verilerin anonimleştirilmesi veya takma adlandırma gibi tekniklerle bu süreç desteklenecektir.

İlgili içeriğe buradan ulaşabilirsiniz.

Ekibimiz

Av. Tuğçe Gültekin
EY Türkiye Hukuk Bölümü Şirket Ortağı

tugce.gultekin@tr.ey.com

Av. Seda İlik Obut
EY Türkiye Hukuk Bölümü Müdürü

seda.ilik@tr.ey.com

EY | Daha iyi bir çalışma dünyası oluşturuyoruz

EY olarak, müşterilerimiz, çalışanlarımız, toplum ve dünyamız için değer yaratırken sermaye piyasalarında güveni inşa ediyor ve bu şekilde daha iyi bir çalışma dünyası oluşturuyoruz.

Veri, yapay zekâ ve ileri teknolojiden yararlanarak müşterilerimizin geleceği güvenle şekillendirmesine, günümüzde ve gelecekte karşılaşabilecekleri sorunlara çözüm üretmelerine yardımcı oluyoruz.

EY ekipleri olarak bağımsız denetim, danışmanlık, güvence, hukuk, kurumsal finansman, strateji ve vergi hizmetleri sunuyoruz. Dünya çapında 150'den fazla ülkede, küresel ağımız, kapsamlı iş birliklerimiz ve güçlü sektörel deneyimizle müşterilerimize hizmet veriyoruz.

Hep birlikte geleceği güvenle şekillendiriyoruz.

ey.com/tr

linkedin.com/ernstandyoung
instagram.com/eyturkiye
x.com/EY_Turkiye
facebook.com/ErnstYoungTurkiye

Shape the future with confidence